

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1. (Currently Amended) A method of managing security keys generated from [[an]] a tree-structured ancestral hierarchy and issued by or on behalf of a service provider in order to provide selective access to provision of a service, wherein invalidation of a key necessitates reconfiguration of each other key within the hierarchy to the extent another key and an invalidated key share common ancestry, the method comprising the steps of:

defining at least two groups of users of the service;

allocating within the hierarchy a distinct subtree domain for each group of users; and

issuing keys to users from subtrees domains within the hierarchy upon the basis of their grouping.

2. (Original) A method according to claim 1 wherein the at least two groups of users are defined upon the basis of a predetermined policy which provides that users are grouped according to their perceived value to a provider of the service.

3. (Currently Amended) A method according to claim 2 wherein a first user group having the highest perceived value to the provider are allocated keys from a first subtree domain, and wherein keys from the first subtree domain share fewer ancestors with keys from other subtrees domains than said keys from other subtrees domains share with each other.

4. (Currently Amended) A method according to claim 3 wherein keys from the first subtree domain share only one ancestor with said keys from other subtrees domains.

5. (Original) A method according to claim 1 wherein the ancestral hierarchy has a binary tree architecture.

6. (Currently Amended) A method according to claim 1 wherein the at least two groups of users are defined upon the basis of a predetermined policy which provides that users are grouped according to a perceived susceptibility of them ceasing to require the service, and a first user group having the highest perceived susceptibility are allocated keys from a first subtree domain, and wherein keys from the first subtree domain share fewer ancestors with keys from other subtrees domains than said keys from other subtrees domains share with each other.

7. (Currently Amended) A method according to claim 6 wherein keys from the first subtree domain share only one ancestor with said keys from other subtrees domains.

8. (Previously Presented) A method according to claim 1 wherein varying levels of service are available and a group of users of a low-service level are allocated dummy keys providing no security, thereby to obviate a need to reconfigure other user's keys upon their invalidation.

9. (Original) A method according to claim 8 wherein the service is a dynamic service and its value is ephemeral and based upon its contemporaneous nature.

10. (Previously Presented) A method of managing security key distribution to a plurality of users of a service comprising the steps of:

defining levels of service provision;

allocating keys to users which are indicative to a service provider of the level of service to which they are entitled; and

for at least one level of service provision, allocating dummy keys which do not provide security for the provision of the service.

11. (Previously Presented) A method according to claim 10 wherein the placebo keys operate in such a manner that a user is not able to perceive a difference between a functioning security key and a dummy key.

12. (Original) A method according to claim 10 wherein the service is dynamic and its value is ephemeral and based upon its contemporaneous nature.

13. (Currently Amended) A computing entity adapted to manage distribution of security keys generated from [[an]] a tree-structured ancestral hierarchy and issued by or on behalf of a service provider in order to provide selective access to provision of a service, wherein invalidation of a key necessitates reconfiguration of each other key within the hierarchy to the extent another key and an invalidated key share common ancestry, the entity being adapted to:

define at least two groups of users of the service;

allocate within the hierarchy a distinct subtree ~~domain~~ for each group of users;

and

issue keys to users from subtrees ~~domains~~ within the hierarchy upon the basis of their grouping.

14. (Previously Presented) A computing entity adapted to manage security key distribution to a plurality of users of a service by:

defining levels of service provision;

allocating keys to users which are indicative to a service provider of the level of service to which they are entitled; and

for at least one level of service provision, allocating dummy keys which do not provide security for the provision of the service.